2010

Mitigating Cyber-Threats Through Public-Private Partnerships: Low Cost Governance with High-Impact Returns

David M. Cook
Edith Cowan University

Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

MITIGATING CYBER-THREATS THROUGH PUBLIC-PRIVATE PARTNERSHIPS: LOW COST GOVERNANCE WITH HIGH-IMPACT RETURNS

David M Cook

secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
d.cook@ecu.edu.au

Abstract

The realization that cyber threats can cause the same devastation to a country as physical security risks has taken the long route towards acceptance. Governments and businesses have thrown the glove of responsibility back and forth on numerous occasions, with government agencies citing the need for private enterprise to take up the mantle, and Business returning the gesture by proposing a 'national' perspective on cyber security. Ambit claims such as these drain a range of security resources when both sides should work in concert by directing all available energy towards resolving cyber-threats. This paper compares the public-private arrangements through Australasia in arguing the need for new modes of governance across cyber-security initiatives. Whilst critical infrastructure partnerships accept the need for joint operations – the broader information technology (IT) security industry has yet to embrace the same.

Keywords: Governance, Public Private Partnerships, Critical Infrastructure, New Modes of Governance, Non Government Organisations

INTRODUCTION

First impressions about the direction of, and responsibility for, cyber security usually focus on governments. They are expected to defend, respond and engage with any and all cyber threats regardless of size and scale. In terms of priorities, governments make no secret of the order in which they choose to act. Critical Infrastructure (CI) remains the number one priority on the basis that CI represents vital organisations, supply chains, information technologies and communications systems. These systems, if wiped out, corrupted or rendered unavailable for an extended period, "would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security" (AGD, 2008, p.3). However, there is also increasing support for the notion that critical infrastructure protection has a broader meaning than the security of nationally important utilities and the essential services of supply, law and order, and communications. The distinction then falls from one of criticality to one of vitality. In this sense the protection of Australian business assets takes on a broader strategy that drives a 'structured approach' to security closely tied to ISO 27001 (APS, 2009). As the national focus shifts from just 'protection' to also include 'resilience', so government policy looks more closely at sharing the wider responsibility for security with both the general business community, and individual consumers.

PRIVATE SECTOR DISCONNECT

Whilst governments are coming to an understanding about the need for the private sector to share some of the communal burden for cyber resilience, the private sector does not collectively share the same sentiment. Certainly there are areas where the two come together successfully, such as specialist security areas including Supervisory Control and Data Acquisition (SCADA) systems (AGD, 2009) and Money Laundering crime prevention through AUSTRAC and its association with the Asia/Pacific Group APG (AUSTRAC, 2008). However, the overwhelming majority of private businesses, as well as general home consumers and individuals, remain agnostic to notions of shared security responsibility, and apathetic towards initiatives that look to draw their involvement closer to government cyber security policy.

This disconnect reveals two specific problems. Firstly, unless a company or organisation has a direct and regular connection with a clearly defined area of Critical Infrastructure Protection, it will actively promote its own governance, culture, and profit stratagem to represent its own best interests. In general, other companies

will not recognise any sense of urgency or priority to cyber security unless they are reacting to a security issue that directly affects their operations. In a nutshell, private companies will not endorse their primary objective as the cyber security of the community and the nation. It is hard to disagree with most commercially-driven enterprise motives that look to protect their shareholders over and above the greater good, especially when corporate company laws, as well as taxation benefits, both funnel each organisation towards their own profit-based directions. The challenge is therefore not to remove a company's prime directive in terms of bottom line profits, but to see how closely the notion of shared responsibility can be elevated behind that prime directive (Groebel, Metze-Mangold, Van der Peet and Ward, 2001). Once profit sharing and cyber resilience shares some of the same corporate attention, the closer each organisation will move towards a system whereby cyber resilience is embedded in the core values and goals of each group.

The second problem is how to get individuals, home users, and small groups to see the value in sharing responsibility for cyber resilience. This second cohort is not a defined group as such, which illustrates the inherent nature of this problem. Individuals and small associations act in their own self interests without any highly developed sense of a larger responsibility, nor any understanding of the value of their potential contribution to the issue. Unlike the general business community, individuals have even greater disconnect from cyber resilience responsibility because they have no sense of Corporate Social Responsibility (CSR). "For corporate responsibility to survive and indeed succeed in Australia, companies must be open to, and seek input from, a broad array of stakeholders, such as its employees, its customers and the community in which it operates" (Kinley, Nolan and Zerial, 2007, p.41). At the same time individual perceptions of responsibility are so diffuse from the specific requisites of cyber resilience that they are lost against a backdrop of many other needs and responsibilities (Budd and Harris, 2009). Together, these two problems stand as thorns in any national strategy to successfully deploy a coherent and integrated approach to cyber resilience.

COMPANIES LOOKING BEYOND INTERNAL GOVERNANCE FRAMEWORKS

At first glance the expectation that a company might look outside its own corporate command and directive substructure is difficult to reconcile with standard business practice. Unless there is specific legislation that compels a firm to devote resources towards cyber security it will only dispense the bare minimum of effort and capital to security. Some firms cooperate but the majority do not. Companies are driven by the desire to generate profits. Cyber security is often seen as an over-exaggerated threat, an unnecessary expense, and a hazard that usually occurs in someone else's organisation (Schneider and Hyner, 2006). Cyber security is therefore often perceived as a 'cost of business', and something that constrains the company's ability to generate profits.

This discrimination is further exacerbated by internal corporate management structures that position cyber security as a technical problem instead of an operations and management problem. Key cyber security strategies are often put forward by IT technical staff who lack the internal stature and the corporate skills to successfully articulate a case and subsequently garner wide spread support from upper management. Cyber security is viewed from a perspective of isolated incidents, and one-off occurrences. It is not seen as an ongoing process but rather as something applied once to 'fix' a problem. This perspective is evident in both businesses and with individuals. In the home, SoHo (small office/home office) users apply antivirus software as if it were a once-only medicine with a cure-all success rate. In larger firms management have a similar expectation, often ignoring technical security and IT staff who prescribe a need for ongoing updates, ongoing patching, and ongoing vigilance. Little wonder then, that cyber resilience fails to gain a foothold in an area of enormously widespread cyber vulnerability.

At the other end of the cyber-ignorance spectrum, specialist utility organisations such as energy providers, water supplies, transport vendors and communications specialists have now developed a highly informed network of practitioners, government agencies and vendors in order to operate secure, robust, and buoyant information and communication technologies as the enabling backbones of their business endeavours. This development of shared responsibilities did not arrive suddenly, but rather from a commitment by government to enter in a range of partnerships that sought to engage businesses especially in areas of critical infrastructure supply, in order to deliver a unified approach to cyber security and cyber resilience in Australia. At the heart of this approach is the building of trust between government and private organisations, and the agreement of those professionals who value the sharing of information for the purpose of maintaining a strong unified approach to security.

Whilst there are still those who retain a somewhat faithless stance to cyber resilience within critical utility provision, the great majority of both technical and management based personnel have an informed understanding of the ongoing need for cyber resilience. The Trusted Information Sharing Networks (TISN, 2008) along with their associated Communities of Interest (COIs) have ensured that this cooperative culture

continues to flourish even though those participating remain wary of shared information that could lead to the competitive advantage of an adversary (AGD, 2008). By building trust and by establishing the practice of public-private partnerships to develop and consolidate security strategies, the cyber security of critical infrastructure, and its associated requisites, has become an important cornerstone of the Australian cyber security strategy.

CYBER RESILIENCE OWNERSHIP

Developing a similarly robust and participatory engagement with the wider business community (along the same lines as those involved in CI) is a difficult proposition. The broad spectrum of businesses must now look beyond their internal governance if they are to accept the mantle of corporately responsible entities. Yet most would not accept the key premise that underscores the arrangement between government and critical infrastructure. Getting those in the business of CI to take ownership of critical infrastructure protection is a task that carries an implied obligation by both government and private enterprise. There is a valid reason to develop partnerships and systems of trust. In the wider business community the acceptance for a shared obligation to security is less established. In its place is a history of indifference with the private sector assuming that Government will protect them in the event of each and every emerging cyber threat. The response so far from the private sector has, in general, been one of reaction rather than pro-action.

In the case of individual actors and many small businesses and associations, there is even less connection to the notion of ownership of the cyber-resilience objective. These smaller concerns may not even see themselves as having any contributing role in cyber security, instead believing that they have no role at all, or otherwise solely as victims rather than partners in a jointly empowering effort to tackle and mitigate the threats of cyber attack. Such is the lack of any cohesive security understanding that the problem of cyber resilience at the consumer level struggles to even identify those who should be partners, let alone those who would be leaders in such an undertaking. Where critical infrastructure protection draws like-minded professionals towards the shared goal of security, the cyber resilience of the wider disparate consumer audience flounders to find commonalities, strengths, or a singular sense of purpose.

Notwithstanding the general mission that the Australian Government through CERT looks to place within business (CERT, 2010), there is another notable disconnect to contend with. Business firms, private organisations, and individual consumers all remain suspicious of government authorities. In an information-sharing age where knowledge is money, it is ironic that the very participants that the Australian government seeks to engage remain cautious of sharing information because there is a perception of possible abuse of trust by government agencies. The perception is that this occurs on two levels. Firstly concern arises that government departments might pass on information to other departments that might lead to incrimination or an infringement. Secondly, that at least some departments and agencies are so involved in the business of cyber security that they may be engaged in spying upon the very businesses and individual consumers that they are trying to engage with. This means that even in businesses that believe in their own internal governance and support a culture that works towards the greater common ideals of cyber resilience there remains a hesitancy to connect with the shared governance (and shared cyber resilience policies) of the nation.

A NEW APPROACH

There is a need for a shift in the approach to governance. This is in terms of governance rather than in terms of engagement because it is the rules, and their associated hierarchy of authority that strike at the heart of the disengagement between consumers and government. Government is perceived to have the upper hand in terms of governance. A federal authority would surely trump that of an individual or a small firm. To achieve a level of true connection in terms of partnership at least one of the major contributing factors is a level playing field upon which the rules and hierarchy of engagement are established and played out. A new mode of governance is required, and it needs to find broad satisfaction throughout the community regardless of scale.

In examining the success of the TISNs and COIs there has been some effort to provide engagement regardless of size or scale. That has been effective to some degree, with regional utility providers enjoying participation alongside much bigger corporations who maintain “giant” status in terms of both revenue and criticality. The issue of criticality does have an impact on the nature of the participation amongst trusted sharing environments. The result is that there is a certain degree of proportional “nesting” of scales. In essence this manifests itself as a greater level of sharing and commonality between CI providers at the giant level, and a sharing of information and cooperation amongst smaller and regional actors. Given that nesting affects participants in critical infrastructure protection networks, one assumes that a similar problem will emerge with the wider business

community and individual consumers. With so much hinging on the need to accept and trust other participants from across a multi-scalar domain, and to engage in open-ended trust and sharing of information, the requirement for a system of governance that accommodates these characteristics looms high on the cyber resilience agenda.

New Modes of Governance (NMG) have proven to be an effective rules framework for the facilitation for public-private partnerships because they are multiscalar and less vertically hierarchical than other forms of governance (Walters, 2004). NMG attracts those difficult to convince participants in networks of trust and sharing predominantly because it resists the temptation to overlay hierarchy from above (Sassen 2003, Rhodes 1996). In its place NMG develops its rules and agreements from a much more socially inclusive system whereby any and all participants share knowledge with both hierarchical and regulatory impunity (Sassen, 2003). This is an important consideration because much of the reluctance by the wider business community is sustained by the notion that information that is shared outside of an organisation may lead to regulatory consequences arising from governance-related misconduct. In simple terms there remains a degree of mistrust between commercial parties, each other, and government.

However the wider appeal of new modes of governance is due to its ability to join small and large groups, organisations and individuals, and government and private sector actors regardless of scale or reputation (Latham and Sassen, 2005). NMG engages actors into largely even platforms, dragging away stereo-typical reactions to cyber security, and laying down simple principles that are highly participatory and conducive for multiple contributing sources that include complex discourse across wide-ranging security positions. Within the context of a vast knowledge-hungry security audience the emphasis is on engagement by as many different means as possible. NMG provides just such a multi-sectoral environment. It removes many of the threats and doubts of actors wishing to engage by passing much of the authority to engage back to the participants rather than expecting them to gather under the rules of an organisation that they do not trust.

The “new modes” approach presumes that there is the need to break down the historical reliance on the Government creation of all rules. The assumption that “government knows best” might have some purchase in areas of previous government ownership. Governments can therefore legitimately lay claim to expertise and experience in the delivery of critical utilities and their associated infrastructure, but this legitimacy does not translate across to the wider business domain, nor does it hold credence amongst individual consumers. Governance, of course, is much more complex than simply creating a system of rules. For the governance to be accepted it has to be accepted by its wider audience. Such an acceptance is dependent upon a raft of conditions being met, including issues of trust, participation, justice and most importantly shared values. Critical infrastructure protection has at its core an acknowledgement of the shared urgency of cyber security (Pfleeger and Pfleeger, 2007). Amongst wider business and individual consumers that urgency is not shared, but rather is a fractured notion that gains a foothold here and there, but does not stand a solid foundation of shared acceptance of a role in cyber security. The question remains, therefore, what factors might be deployed in order to create such a shared undertaking and adoption of values?

PUBLIC-PRIVATE PARTNERSHIPS

From an ICT perspective, most large scale private firms are substantially more efficient at processes and systems than their public sector counterparts (IPA, 2007). As government policy more fervently continues to cite the need for a state of preparedness against cyber attack, private enterprise considers itself better prepared than the government’s assertion, and discounts the need for a greater shared understanding of cyber resilience. On the one hand the public sector wants to tell the private sector what rules to follow in order to align with the national understanding of resilient preparedness, whilst on the other hand the private sector looks to its shareholders first, and its colleagues in government last. Private firms are not very adept at seeing the need for governance from outside their own firms, especially when key decisions might be played out externally to each firm’s own set of boundaries. This is the dilemma of shared governance when applied instead of hard legislation. In a ‘carrot and stick’ environment the ‘stick’ forces those being struck to do the least possible in order to comply, whilst the ‘carrot’ forces the same people to question: “why aren’t you hitting me with a stick?”. In conditions such as these public-private partnerships (PPPs) bring public and private parties together and avoid the uncertainty of misunderstandings about motives. PPPs have clear objectives and describe business interests and policy objectives with significantly greater clarity.

With this in mind, the need for public-private partnerships that develop cyber security and recovery in the general business community, as well as with individual consumers, emerges as the option of best fit for governments in pursuit of a broad-based cyber resilience strategy (Furnell, 2002). PPPs are no longer seen as

the undesirable, unprofitable project partnerships they were previously viewed as. Recent government commitments have seen a range of PPPs emerge that touch on areas relating to, and benefiting directly from, cyber resilience. In recent years, the Computer Network Vulnerability Assessment (CNVA) programs devised and co-funded by the Attorney General's Department is perhaps the most noteworthy example of a PPP in this area (AGD, 2009). Focusing on the security of networks and systems within private organisations involved in critical infrastructure delivery, the CNVA program successfully shone the spotlight over CI security with a deliberate emphasis on cyber security. The program showed the benefits of PPPs as solutions in the area of cyber resilience. CNVAs were neither prescriptive, nor were they heavily legislative. Instead, they actively encouraged industry to examine their internal security vulnerabilities through third party investigation and first party cooperation. CNVAs are expensive exercises and examinations of this kind are often bypassed on the basis of a commercial rationale. Unfortunately that commercial reasoning was often based on the oversimplification of an internal risk assessment that ranked cyber vulnerabilities very lowly on the basis of little or no previously damaging attack history. CNVAs were instrumental in raising awareness to a much greater understanding of consequence, and to demonstrating specific internal threats and their likelihood, consequence and impact on both the firm and national CI.

In 2010 the National Broadband Network (NBN) looms as the single biggest Public Private Partnership ever undertaken by the Australian government (AGD, 2010). It will draw commercial activity across cyber issues on a scale never before encountered on the Australian landscape. With that broad-based undertaking comes a new wave of cyber vulnerability, spawned by greater bandwidth, faster download times, and wider interaction by the general business community and individual consumers. Whilst the NBN will bring high speed internet to more homes and businesses than ever before, there is, as yet, no corresponding security strategy that is aimed to match these developments in anywhere near the same size and scale. The time is clearly right for PPPs to engage with ordinary business and with individual consumers.

This paper has already explained the significant differentiation between hard-core CI business, and the wider commercial activities of ordinary business and home-based consumers. The former now has a razor-sharp approach to cyber resilience, whilst the latter has at best a blunted and blurred understanding, and at worst is ignorant in the extreme. The key research question looms as to what kind of PPPs might best connect these diverse 'cyber-participants', and how best to overcome the previously cited problems of trust, information sharing, and commercial best- practice.

RESILIENCE STRATEGIES FROM UNLIKELY SOURCES

The wider success of resilience strategies comes from a set of unlikely sources. In South-east Asia critical infrastructure has taken a much greater hammering from natural disasters than from deliberate attacks. Nevertheless, through bitter experience the resilience approach to CI in many less-developed nations serves to illustrate possible pathways and collaborative partnerships that have previously been ignored within Australia. In Indonesia, the dominant CI questions arise from experience with both natural disasters and terrorist attacks. The Republic of Indonesia has a heightened sense of resilience based on decades of natural events including volcanic eruptions, floods, monsoons, tsunamis, and earthquakes. Similarly, Indonesia has a decade of experience with attacks on physical infrastructure from terrorists, with the result that regional critical infrastructure protection and its associated strategies is at an all time high. In response to these regional CI characteristics, both Indonesia and Singapore demonstrate strategies towards greater resilience that are useful in mapping some possible solutions to Australia's dilemma of integrating cyber resilience to the general business and individual consumer communities.

Most robust CI solutions come about through necessity. In the south-east Asian region terrorist-driven as well as natural disaster-resilient strategies for overcoming issues in supply have emerged from an assortment of partners. Indonesia has witnessed first-hand the deployment of Non-Government Organisations (NGOs) and their various development programs. A history of misfortune in both natural and terrorist disasters has translated to many ongoing resilience-building tactics and programs from international NGOs. Programs by the Red Cross, the World Bank, the United Nations, and the OMG big group, find enormous acceptance because they combine a solutions-based approaches to problems of urgent need. They also gain widespread community acceptance (social capital) by capturing the support of the grassroots public. Indonesian citizens in Central Java now pass information through to authorities about known associates of terrorists because they have an appreciation of the value of the wider community safety and well being that overrides their previous suspicions of Indonesian police, military and law enforcement (LE) (TISN, 2010). Ardent Muslims in Aceh embrace joint health programs between the Red Cross and the Red Crescent (despite previous mistrust of Christian doctors in the Red Cross) because they understand the value of community health and the speed with which ignored health

programs translate to illness, death and widespread misery (UNPAN, 2004). Reconstruction of critical airport infrastructure in post-earthquake Yogyakarta from World Bank funding gains community support because it partners with local businesses across a range of demolition and construction skills and services (JRF, 2007).

Non Government organisations make excellent associates for PPPs because they work at the grass roots of the community in which their arrangements are meant to operate, and because they include the sense of human "urgency" that carries both legitimacy and appeal in such a way that it draws in community involvement. The disengagement between the Australian Government and the wider business community in terms of cyber resilience endures a lack of this legitimacy and appeal. How can the wider business community, along with the enormous number of individual consumers, become drawn to practices that are cyber resilient unless they sense that same human "urgency" that occurs under the operating conditions of the World Bank. The Red Cross, and hundreds of other NGOs?

The answer lies in finding NGOs that function within an "urgent" and "passionate" culture. Doctors, nurses and health workers volunteer time and devotion in times of crisis to the Red Cross. This is underscored by long-term deployments in areas of need. In some cases that manifests itself in the form of living and working in third world countries. In other cases it shows up as work in blood banks in local cities. In each case they are driven to action because there is a sense of urgency, and a culture that fosters a sense of duty and obligation. Who are the NGOs of the internet? Why are they harder to identify and how can they be convinced to evince the same urgency, duty and obligation that shows up in the cyber resilience of traditional critical infrastructure such as energy, water and utilities? The answer to these questions lies in forming public-private partnerships that generate the same cultural urgencies as those best seen in international NGOs. PPPs draw parties together under two key elements. The first is the need for change and development, and the second is the demand for a commercial imperative.

In Australia there are several organizations that operate as quasi-NGOs, but function on a shoestring. The Australian Computer Society (ACS) has a Code of Practice that states that it must safeguard the interests of members and their clients (individual consumers) in both legislative and social terms (ACS, 2009a). The ACS already performs a range of other "NGO-like" services in terms of its engagement with graduates, assistance with working visas and student visas for international students, and its involvement with "Skilled Migration" as IT Professionals (ACS, 2009b). Yet in the area of skilled migration and working visas there is no clearly "urgent" catalyst that drives the same imperatives that are needed to operate widespread cyber resilience.

For an organisation to accept the title of NGO in its more globalised social sense there is still a need for a much greater depth of community service and social benefit. In most cases, that service is delivered through a highly organized approach to project management. In the case of the ACS, the requisite synergies could not be stronger. The ACS actively promotes project management and incorporates it into many of its programs and engagements. The missing elements are the same as the two functional components of PPPs, the need for the development and the need for the commercial "survival" to drive the development.

There is of course, a third reason why NGOs emerge in the first place. This is because the private sector cannot bring itself to engage in a particular area because it is economically unappealing to the point of detracting from the core business of a firm. Anti-Virus software companies exist to make a profit from selling their software, just as Pharmaceutical companies exist to profit from selling their medicines. Yet neither the big pharmaceuticals nor the big AV companies take on the role of development and community service that is required in the face of urgent need. NGOs are therefore often an important link between areas of developmental need and areas where there is insufficiently high levels of profit to sustain commercial involvement and dominance of that development.

Public-Private Partnerships have re-emerged on the Australian business landscape as a method of delivering CI strategy into areas where fully-developed critical infrastructure protection is retarded by private commercial consideration, issues of privacy, trust, and executive ignorance. Governments are now more attracted to PPPs than other traditional forms of procurement for two important reasons. Firstly, PPPs exist in project form. They have a definite beginning date and a definite end date. This means that they represent a measurable approach to a specific problem and bring about a reportable result within a similar (or shorter) timeframe than other procurement methods. From this perspective, PPPs have political appeal since they can be tailored to fit specific time frames in line with electoral expectations (IPA, 2007). Secondly, PPPs are more cost effective and time efficient than other procurement systems because they maximize market competition and operate efficiently regardless of size and scale (English, 2005). PPPs are now the preferred method for critical infrastructure

development and have moved beyond traditional physical CI into areas of awareness, education, and cultural development.

In particular, CIP in the broad sense is more susceptible to information and influence. Information operations therefore have a much closer relationship with the wider business community in addressing the need for this community to respond to the wider set of vulnerabilities and threats. Whereas issues that undermine the public confidence have previously rested on the shoulders of energy, security and utilities-based critical infrastructure there is new and growing demand to protect the next lower (and broader) tier of services and organisations that are still vulnerability to a range of threats and vulnerabilities. In one sense therefore, the use of an organisation with NGO status enables a PPP to succeed over traditional public sector development because the NGO already has a trust relationship with the business community and at least partial connection with individual consumers. In the case of the ACS their extensive membership and organizational networks represent significant development assets in the deployment of cyber resilience. By using a PPP of this kind, new modes of governance emerge as an effective carriage in connecting with small and general consumers regardless of stature or scale of operation (Hodge and Greve, 2005).

PPPs carry with them a sort of inherent "trust weighting". When viewed in terms of the durability between public and private actors, Van Ham and Koppenjan (2001) note that as resources and services are jointly developed in an environment of shared risk, there is an implicit trust that develops that is in proportion to the shared risk. In other words, governments are able to foster trust by means of shared financial and social risk. Again, new modes of governance become the enabling rules framework of choice because they allow significantly greater participation that places asymmetrically positioned partners in contact with small scale individuals and businesses in a single partnered development proposition (Pollitt, 2005).

CONCLUSION

Cyber security is at least partially a concept rather than a tangible object. It carries the combined burdens of mistrust, ignorance, inefficiencies, and misunderstanding. Governments make poor enablers of cyber resilience unless partnered with associations that engage across all burdens, into business and individual environments of any size, and amongst networks where there is a commonly shared and believed commercial imperative. The need for PPPs in the deployment of cyber resilience goes beyond simply partnering with a company. To successfully engage a widespread audience of individual consumers and small scale business operators such a partnership needs the added status of urgency across the critical infrastructure sphere of influence. In developing nations where CI issues carry urgency into every corner, and the issues of the day centre around trust information sharing, NGOs emerge as the partners of choice. They naturally operate within new modes of governance and overcome partnership issues that are constrained by heavy handed hierarchies. The challenge for the Australian government is to select an association that emulates these characteristics. Such an organisation would have sufficient connection to the target community, whilst also demonstrating enough urgency to the topic of cyber security.

This paper has referred to the Australian Computer Society as a possible association for engaging in a Public-Private Partnership with the Australian government to deploy cyber resilience down to the level of individual consumers. Other NGOs and IT associations may be equally if not better suited. Whatever the choice, the choice of partner remains unresolved. In positing the possible use of NGOs to create urgency in consumer CI, this paper underscores the need for further modeling and research into the right kind of partnerships to secure the cyber resilience of the wider community.

REFERENCES

ACS (2009a) Code of Professional Conduct and Professional Practice, Australian Computer Society; Retrieved 30th June 2010 from http://www.acs.org.au/index.cfm?action=show&conID=copc2#A1

ACS (2009b) Pre Application Skills Assessment (PASA). Australian Computer Society; Retrieved 3rd July 2010 from http://www.acs.org.au/index.cfm?action=show&conID=skillassessment

AGD (2008) Critical Infrastructure Protection, Attorney Generals Department; Retrieved 21st March 2009 from http://www.ag.gov.au/www/agd/agd.nsf/Page?Nationalsecurity_CriticalInfrastructureProtection/2008/

AGD (2009) Computer Network Vulnerability Assessment Program, Attorney-General's Department; Retrieved 21st June 2009 from

http://www.ag.gov.au/www/agd/agd.nsf/Page/GovCERT_ComputerNetworkVulnerabilityAssessmentProgram

AGD (2010) Cyber Security Strategy, Attorney Generals Department; Retrieved 29th July 2010 from http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

APS (2009) Australian Government Protective Security Manual, Australian Public Service Commission; Retrieved 3rd July 2010 from http://www.apsc.gov.au/foundations/security.htm

AUSTRAC (2008) Asia/Pacific Group on Money Laundering, Australian Transaction Reports and Analysis Centre; Retrieved 4th July 2010 from http://www.austrac.gov.au/multilateral_engagement.html

Budd, L. and Harris, L. (2009) "Managing Governance or Governance Management. Is it all in a Digital Day's Work?", in L.Budd & L.Harris (Eds.), E-Governance: Managing or Governing? New York: Routledge.

CERT (2010) Industry Engagement, CERT Australia, Australia's National Computer Emergency Response Team; Retrieved 3rd July from http://www.cert.gov.au/www/cert/cert.nsf/Page/Industry_Engagement

English, L. (2005) Using public-private partnerships to deliver social infrastructure: the Australian experience, pp290 – 304 in Graeme Hodge and Cartsen Greve (eds) The Challenge of Public-Private Partnerships: Learning from International Experience, Edward Elgar, Cheltenham, UK, and Northampton, MA, USA.

Furnell, S. (2002) Cybercrime: Vandalizing the Information Society, London: Adison-Wesley

Groebel, J., Metze-Mangold, V., Van der Peet, J., and Ward, D, (2001)Twilight Zones, in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, Bonn: Friedrich-Ebert-Stiftung.

Hodge, G., and Greve, C. (2005) Public-Private Partnerships: An International Performance Review, Public Administration Review, Vol 67, No. 3, May/June, pp 545–558.

IPA (2007) Performance of PPPs and Traditional Procurement in Australia, Final Report to Infrastructure Partnerships Australia, Allen Consulting Group, Melbourne Victoria: Retrieved 3rd July from http://www.infrastructure.org.au/content/PPP.aspx

JRF (2007) One Year after the Java Earthquake and Tsunami: Reconstruction Achievement and the Results of the Java Reconstruction Fund, Java Reconstruction Fund, Retrieved 5th March 2010 from http://www.javareconstructionfund.org/ducuments/pdf/progresreportjrf_062007.pdf

Kinley, D., Nolan, J., and Zerial, N. (2007) The Politics of Corporate Social Responsibility: Reflections on the United Nations Human Rights Norms for Corporations, Sydney Centre for International Law, Faculty of Law, University of Sydney Working Paper no.8 February 2007, Retrieved 3rd July from http://sydney.edu.au/law/scil/documents/2009/SCILWP8.pdf

Latham, R., & Sassen, S. (2005) Digital Formations: Constructing an object of study, in R.Latham and S Sassen (Eds), Digital Formations: IT and New Architecture in the Global Realm. Princeton: Ptrinceton University Press.

Pfleeger, C.P., & Pfleeger, S.L. (2007) Security in Computing. Fourth edition, Boston, Pearson: Prentice Hall.

Pollitt, G. (2005) Learning from the UK Private Finance Initiative Experience., In The Challenge of Public-Private Partnerships: Learning from International Experience. (Eds) Graeme Hodge and Carsten Greve, 207-230. Cheltenham, UK: Edward Elgar.

Rhodes, R.A.W. (1996) "The New Governance: Governing without Government", in Political Studies, 1996, XLIV, pp652-667.

Sassen, S. (2003) Globalisation or denationalization? Review of International Political Economy Vol 10.1, pp1-22

Schneider, V., and Hyner, D. (2006) Security in Cyberspace: Governance by Transnational Policy Networks, in New Modes of Governance in the Global System: Exploring Publicness, Delegation and Inclusiveness, (Eds) Mathias Koenig-Archibugi and Michael Zurn, pp 154 - 174. Basingstoke, UK: Palgrave MacMillan

TISN (2008) Trusted Information Sharing Network for Critical Infrastructure Resilience, Trusted Information Sharing Network (TISN); Retrieved 3rd July 2010 from http://www.tisn.gov.au/www/tisn/content.nsf/Page/Resilience

TISN (2010) CIPMA: Modelling and Analysis, Trusted Information Sharing Network (TISN); Retrieved 3rd July 2010 from http://www.tisn.gov.au/www/tisn/content.nsf/Page/Modelling_and_analysis

UNPAN (2004) NGOs Respond to Asian Tsunamis, United Nations Public Administration Network; Retrieved 6th July 2010 from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN019579.pdf

Walters, W. (2004) "Some critical notes on governance". Studies in Political Economy, Volume 73, pp 25 – 42.